PCT/IB 96/00859
11. 10. 96

Europäisches Patentamt | European Patent Office | Office européen des brevets

08/981461

REC'D 11 OCT 1996
WIPO PCT

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

95113489.9

PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

N.A.S. Kettle

MÜNCHEN, DEN
MUNICH,
MUNICH, LE

12/09/96

EPA/EPO/OEB Form 2540 - 02.91

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 95113489.9

Anmeldetag:
Date of filing:
Date de dépôt: 28/08/95

Anmelder:
Applicant(s):
Demandeur(s):
Feldbau, Ofra
Ramat Gan 52424
ISRAEL

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Apparatus and method for authenticating the dispatch and contents of documents

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
H04L9/32

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/DE/DK/ES/[redacted]/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques: The title of the application as originally filed reads as follows :
" Apparatus and method for authenticating the dispatch of documents"

PCT/IB 96 / 00859
27. 11. 96

8/981461

STATE OF ISRAEL

REC'D 28 NOV 1996
WIPO PCT

זאת לתעודה כי
רצופים בזה העתקים
נכונים של המסמכים
שהופקדו לכתחילה
עם הבקשה לפטנט
לפי הפרטים הרשומים
בעמוד הראשון של
הנספת.

This is to certify that
annexed hereto is a true
copy of the documents as
originally deposited with
the patent application
particulars of which are
specified on the first page
of the annex.

ON THE 7.8.1996

THE APPLICANT REQUESTED LEAVE
TO AMEND THE SPECIFICATION
A TRUE COPY OF THE AMENDED
PAGES MARKED "17234/2"
ATTACHED HERETO.

ביום 7.8.1996

ביקש המבקש לתקן את הפירוט.
העתק נאמן של הדפים
המתוקנים כפי שהם מסומנים
מצורפים בזה. "17234/2"

PRIORITY DOCUMENT

This 31-10-1996 היום

רשם הפטנטים
Registrar of Patents

נתאשר
Certified

חוק הפטנטים, תשכ"ז – 1967
PATENT LAW, 5727 - 1967

בקשה לפטנט
Application for Patent

לשימוש הלשכה
For Office Use

מספר: Number	117234
תאריך: Date	02-02-1996
תוקדם/נדחה Ante/Post-dated	

אני, (שם המבקש, מענו ולגבי גוף מאוגד – מקום התאגדותו)
I (Name and address of applicant, and in case of body corporate-place of incorporation)

Ofra Feldbau
12 Avtalion Street
Ramat Gan 52424

עפרה פלדבאו
רחוב אבטליון 12
רמת גן 52424

Being the Inventor — היותי הממציא

בעל אמצאה מכח ..... ששמה הוא
Owner, by virtue of ..... of an invention the title of which is

מתקן ושיטה לאימות משלוח מסמכים ותוכנם
(בעברית) (Hebrew)

APPARATUS AND METHOD FOR AUTHENTICATING THE DISPATCH AND CONTENTS OF DOCUMENTS
(באנגלית) (English)

מבקש בזאת כי ינתן לי עליה מטנט — hereby apply for a patent to be granted to me in respect thereof.

• דרישה רין קדימה Priority Claim		
מדינת האגוד Convention Country	תאריך Date	מספר/סימן Number/Mark
EP	28 AUG 1995	95113489.9

• בקשת מטנט מוסף – Application for Patent Addition	• בקשת חלוקה – Application of Division
• לבקשה/לפטנט to Patent/Appl.	מבקשת פטנט from Application
No. ..... מס'	No. ..... מס'
dated ..... מיום	d ..... מיום

• יפוי כח: כללי
P.O.A.: general/individual-attached/to be filed later-
filed in case ..... הוגש בענין

המען למסירת מסמכים בישראל
Address for Service in Israel
Dr. Mark Friedman & Co.
Samueloff Building, 7 Haomanim Street
67897 Tel Aviv

חתימת המבקש
Signature of Applicant

This 21 יום בחודש II of the month 1996 שנת of the year

לשימוש הלשכה
For Office Use

Ref. No. 497/4

APPARATUS AND METHOD FOR AUTHENTICATING THE DISPATCH OF DOCUMENTS

FIELD OF THE INVENTION

The present invention relates to a method and apparatus for authenticating the dispatch and the contents of dispatched information in general.

BACKGROUND OF THE INVENTION

Post, courier, forwarding and other mail services, which enable people to exchange documents and data, have been widely used both in the past and at the present time.

With the evolution of modern technology, electronic data interchange (EDI) has become a rapidly developing avenue of communication. The use of EDI devices, such as modems, facsimile machines, electronic mail (E-Mail), computers, communication networks, and so forth, is growing throughout the world.

A substantial quantity of the information exchanged, such as contracts, purchase orders, invoices, monetary orders, notices, and even warning and notification messages, are of utmost importance. Sometimes, when a dispute arises between the sending and receiving party of the exchanged information, the receiving party may raise the claim that he never received the information, that the received information was different from what the sender claims to have sent, or the receiving party may have attempted to forge the received information.

The need, therefore, arises for the sender to prove that specific information has been sent at a specific time to that specific receiving party.

Various solutions to various related problems have been proposed in the literature. For example, the transmission operation itself may be authenticated, as shown in US Patent 5,339,361 (Schwalm et al.), which describes a communication system providing a verification system to identify both the sender and recipient of electronic information as well as an automatic time stamp for delivery of electronic information. This patent, however, does not verify the dispatched information.

Document authentication methods, for example by notarization, have long been in use. A method for notarization of electronic data is provided by US Patent 5,022,080 (Durst et al.) which authenticates that source data has not been altered subsequent to a specific date and time. The method disclosed includes mathematically generating a second unit of data from the first unit of data, as by CRC generation, parity check or checksum. The second unit of data is then encrypted together with a time/date indication, and optionally with other information to form an authentication string. Validation that the first unit of data has not been changed is provided by comparing the original data's authentication string with the authentication string generated from the data and time in question. A method is even suggested for having the recipient verify the authenticity of the sender, the time of transmission and the data.

Other patents which discuss document authentication are U.S. 5,136,646 and 5,136,647 both to Haber et al. According to these patents, a unique digital representation of the document (which is obtained by means of a one-way hash function) is transmitted to an outside agency, where the current time is added to form a receipt. According to patent 5,136,647, the receipt is certified using a public-key signature procedure (i.e. encrypted), and optionally linked to other contemporary such receipts thereby fixing the document's position in the continuum of time. According to patent 5,136,646, the receipt is certified by concatenating and hashing the receipt with the current record catenate certificate which itself is a number obtained by sequential hashing of each prior receipt with the extent catenate certificate.

Proof of delivery of non-electronic documents is provided, for example, by Registered Mail and courier services. It is commonly used to authenticate the delivery of materials at a certain time to a certain party, and serves as admissible proof of delivery in a court of law. However, no proof is provided as to the information contents of the specific dispatch.

E-mail and message forwarding services are commonly used today. The sender sends a message to a central databank which, in turn, forwards the message to the destination and provides the sender with a written report authenticating the delivery itself, which includes the date and time of the dispatch, the recipient's address, the transmission completion status, and sometimes even the number of pages delivered, the recipient's identification information, and so on. Again, the provided delivery authentication report is not associated with the specific contents of the materials included in that specific dispatch, is usually maintained apart from the specific data itself, and mainly serves for accounting purposes. Moreover, no record of the

specific data sent is maintained in the databank after the delivery is completed or provided to the sender.

Electronic information, such as a disk document file, transmitted for example via facsimile or modem, is very difficult to authenticate unless reduced to paper document form, which defeats the purpose of EDI. Moreover, some electronic information such as database or graphic files, are not in readable form (e.g., not in ASCII), and cannot be reduced to paper unless custom printing software is used to print the contents of the file. Furthermore, documents and other information which have been transmitted via facsimile or modem are not admissible evidence in a court of law. Worse yet, if the original is destroyed or lost, the sender has no way to prove what was actually sent.

SUMMARY OF THE PRESENT INVENTION

The literature does not provide a comprehensive solution that directly addresses the problem in question: what information has been sent to whom and when. Accordingly, there is a need for a method and system to provide the sender with a convenient means for authenticating both the dispatch and the contents of documents, electronic information and other information during the normal flow of daily activities.

It is therefore an object of the present invention to improve the capacity of conventional systems and methods for dispatching documents and transmitting information to provide the sender with admissible evidence of the dispatch and its contents.

The present invention discloses a method and apparatus for providing a sender with proof of both the dispatch and the contents of the dispatched materials. The dispatched materials can be paper documents, electronic information or other information which can be dispatched electronically by transmission or non-electronically, such as by courier or registered mail service, to an address of a recipient.

According to the present invention, dispatch related information is associated with the contents of the dispatch, in a relatively secure, or reliable manner. This associated information can be provided for example to the sender, and may serve as an admissible authentication of the dispatch and its contents, for example, in a court of law, and therefore it is collectively referred to herein as the "authentication information".

The present invention encompasses all types of information being dispatched, such as that found on paper documents or within electronic documents and other electronic data, and all types of dispatch methods, such as transmission via facsimile machines, modems, computer networks, electronic mail and so forth, or manually via registered mail or courier services.

The term "the contents of the dispatch" herein refers to any information element having information content the substance of which is equivalent to that of the information being dispatched. This includes for example the information source, either in paper document or electronic form, the actual dispatched information, any copies thereof, and so forth regardless of the representation or form.

The present invention also encompasses all types of methods and apparatuses which provide and/or associate the dispatch information with the contents in a relatively secure or reliable manner. The terms "relatively secure" and "reliable" herein mean "reasonably

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the drawings in which:

Fig. 1 is a schematic pictorial illustration of the authentication method of the present invention implemented in a manual manner;

Fig. 2 is a schematic illustration of an authenticator, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic illustration of an alternative authenticator, constructed and operative in accordance with another preferred embodiment of the present invention;

Fig. 4 is a schematic illustration of an alternative authenticator, constructed and operative in accordance with yet another preferred embodiment of the present invention; and

Figs. 5 and 6 are schematic illustrations of verification mechanisms constructed and operative in accordance with the authenticator of Fig. 4.

tamper-proof" or "tamper-detectable", i.e., that it is assured that the authentic information elements are provided and associated in a reliable manner, for example by a non-interested third party or by a device or by a combination of both, and furthermore, that the associated authentication information is secured against fraudulent actions such as disassociation, modification, replacement etc., attempted by an interested party such as the sending or receiving party, at least such that such actions are detectable.

The dispatch information can be any information describing at least the time and destination of the dispatch and preferably the dispatch completion status. Other information relating to the dispatch, such as the identity of the sender and/or the recipient, handshake information, the actual elapsed dispatch time, the number of pages dispatched and so forth. The identification of the authenticator, for example its name, logo, stamp, etc. can also be provided.

Finally, the authentication information can be secured or stored in a secure location or device, in its entirety or in part, together or separately, as desired.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which illustrates the method of the present invention as it can be implemented for paper documents being sent non-electronically. The method of Fig. 1 can be implemented for documents sent via any document dispatching service, such as a courier service or the registered mail service of the post office.

The sender 10 provides the documents 12 to be sent and a destination address 14 to a clerk 20 of the document dispatching service. The clerk 20 prepares a dispatch sheet 26, which typically has a unique dispatch identifier (not shown) and has room for dispatch information such as the time of dispatch or delivery 16, the destination address 14, an indication 18 of proof of delivery such as the recipient's identity and/or signature, and optionally, additional dispatch information such as the dispatcher's signature and the identity of the sender 10, etc.

The clerk 20 fills in the dispatch sheet 26 with the date/time 16 and the address 14, and then prepares a copy 24 of the documents 12 and a copy 34 of the dispatch sheet 26, typically by utilizing a copy machine 22 or an electronic scanner. The clerk 20 then places the original documents 12 into an envelope 28 carrying the address 14, and sends the envelope 28 to its destination 30. In one embodiment of the present invention the dispatching service utilizes a cash-register like device to fill in the dispatch sheet 26. This provides for reliable time stamping and automated dispatch record keeping. Furthermore, the electronic dispatch information produced by such device can be associated using a special mathematical method as discussed in greater detail hereinbelow.

The clerk 20 associates the copy 24 of the documents 12 with the copy 34 of the dispatch sheet 26 by any method, a few examples of which follow:

a) by inserting the documents copy 24 and the dispatch sheet copy 34 into an envelope 32;

b) by inserting the copy 24 of the documents into an envelope 32 and marking the dispatch identifier on the outside of the envelope 32;

c) by printing the dispatch identifier on the documents copy 24;

or d) attaching the copies 24 and 34 and applying the stamp of the dispatch service in such a manner that part of the stamp is on the copy 24 of the documents and part of the stamp is on the copy 34 of the dispatch sheet 26.

Preferably, the clerk 20 secures the copies 24 and 34 in a manner that makes it difficult to modify or replace the information contained therein, for example by marking the pages of the copy 24 with the dispatching service's signature, stamp or seal, by spreading each page with invisible or other ink, by sealing the envelope 32 or by retaining them in the service's secure file 36 and so forth.

In one embodiment of the present invention, the associated copies 24 and 34 are provided to the sender at this stage (where the dispatch sheet 26 is retained with the service to ascertain delivery and to fill in the proof of delivery indication 18) or after the delivery is completed. In another embodiment, the dispatch service retains, in a secure location 36, one or both of the copies 24 and 34.

The clerk 20 can also identify the authenticating party, for example via his signature, or by having the dispatch sheet copy 34 printed on the stationary of the dispatching service, by stamping the documents and/or dispatch sheet copies with the service's stamp, logo or seal, etc.

When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. The envelope 32 therefore, provides a reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.

It will be appreciated that, since a non-interested third party who is neither the sender nor the receiver copied the original documents 12 being sent, it is unlikely that the copies stored in the envelope 32 are other than copies of the original documents 12.

Various modifications can be made to the embodiment provided hereinabove without departing from the scope and spirit of the present invention. For example, the document copy could be sent to the destination while the original could be authenticated. The authentication information could be provided by the service, directly to the court of law. The document copy could be produced by a scanner or a camera and stored in an electronic or other storage device such as a disk or on microfilm, while a copy thereof is provided to the sender. The original dispatch sheet could be first filled out and then provided to the sender instead of using a copy. Moreover, the original documents could be scanned by the sender in the

service's premises into a secure disk and one printed copy thereof could be sent by the service to the destination while another copy could be authenticated and provided to the sender. In the case of a courier, the courier could produce the copy himself using a photocopier at the sender's premises, and so forth.

Reference is now made to Fig. 2 which illustrates an authenticator 70, constructed and operative in accordance with a preferred embodiment of the present invention, which can be part of a system for transmitting information, whether by facsimile machine, modem, computer, network or E-Mail stations, and any combinations thereof, or by other electronic means.

Fig. 2 illustrates a data communication system comprising a sending transceiver 42, a communication line 45, coupled to the sending transceiver 42, a communication network 44 and a receiving transceiver 46. Authenticator 70 of the present invention communicates at least with the sending transceiver 42, and can form part of the sending transceiver 42 or can be separated therefrom.

The sender provides original materials 40 for transmission, which can be paper documents or electronic information such as computer disk, memory and other electronic information including audio/video, text and graphics files or pictures. The sender also provides the destination address 52 which represents the address of the receiving transceiver 46 on communication network 44. The address 52 may for example be a dial number, a network user code and so forth. The sending transceiver 42 needs to transmit the information contents of the materials 40 to the receiving transceiver 46. To provide authentication, the transmission in Fig. 2 is performed through the authenticator 70 in a "store & forward" manner.

The authenticator 70 comprises input means 72 for receiving the transmitted information 60 and the destination address 62 from the communication line 45. The input means 72 may for example comprise a line interface, a Dual-Tone Multi Frequency (DTMF) decoder for receiving a destination address 62 such as a dial number, and a transceiver similar to that of the sending transceiver 42 which can receive the information 60.

The authenticator 70 also comprises an optional storage unit 54 such as a tape, disk or memory device and so forth for storing the information 60 and related dispatch information, an internal clock 50 for generating a time indication 66 of the transmission, a transceiver 76 for transmitting the information 60 to address 62 (the transceiver 76 can be used by the input

unit 72 as well, for example by using a relay mechanism), a controller 56, a user interface 48, and an output unit 58 for providing the authentication information, for example to the sender.

The information 60 is then transmitted over the communication network 44 to the receiving transceiver 46 by the transceiver 76 using the address 62.

The internal clock 50 provides an indication 66 of the current time, and is utilized to provide a time indication for the transmission. Internal clock 50 is securable (to ensure the veracity of the produced time indication 66), and preferably provides time indications according to a non-changing time standard, such as Greenwich-Mean-Time (G.M.T.). Alternatively, the time indication 66 can be externally obtained, for example from a communication network server, as long as the source is secured from being set or modified by an interested party such as the sender. The security of the time indication can be provided in a number of ways, such as by factory pre-setting the clock 50 and disabling or password securing the Set Date/Time function of the internal clock 50. Alternatively, the clock 50 can maintain a "true offset" with the true preset date/time, that reflects the offset of the user set date/time from the genuine preset one.

The transmission completion indication 64 provides information regarding the success of the transmission. It is typically obtained from the communication protocol used by the transceiver 76. It may be for example in the form of an electronic signal provided by the transceiver 76 which is used to determine the validity of the rest of authentication information, or in a form similar to that provided in transmission reports such as "TRANSMISSION OK" or "ERROR". In one embodiment of the present invention, the fact that the rest of authentication information elements are provided, indicates that an affirmative completion indication has been provided.

The storage unit 54 is used for storing the information 60 and/or the dispatch information, including the address 62, the time indication 66, and optionally the transmission completion indication 64. Typically, the storage unit 54 is relatively secure, such that the authentication information contained therein is assumed unchangeable. For example it may be a Write-Once-Read-Many (WORM) device such as an optical disk or a Programmable Read-Only Memory (PROM) device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the authentication information is stored in a secure manner, for example using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by

the widely used RSA encryption method, and by the PKZIP(tm) program from PKWARE Inc., Glendale Wisconsin, U.S.A., and preferably where the "unsecuring" procedure, key or password are unknown to any interested party.

The controller 56 associates the information 60 and the dispatch information, by storing them in storage unit 54 and by associating link information with the stored authentication information, for example in the form of a unique dispatch identifier such as a sequential dispatch number.

To provide the authentication information for the transmission, the dispatch identifier is provided to the controller 56 through the user interface 48. The controller 56, in turn, retrieves the various stored authentication information elements from storage unit 54. If the stored information is also secured (i.e. by compression, password, etc.), the controller 56 "unsecures" them, and then provides them to the output unit 58.

The output unit 58 provides the authentication information to an output device (not shown). The authenticator 70 may include an output device or may communicate with some external unit. The output device can be, for example, a printing unit, a display unit, a storage unit such as a computer disk, the printing apparatus of the sending transceiver 42 and so forth.

The information 60 and the dispatch information, can be associated with each other in any suitable manner. For example, they can be stored in storage unit 54 together (e.g. sequentially or combined into a single file), or separately using a link information element (e.g. using a dispatch identifier). If the output is a printout, output unit 58 typically formats the printout to indicate the dispatch information on at least one, and preferably on all, of the pages containing the printout. Alternatively, a link information element, such as a dispatch identifier, can be printed on each printed page of the information 60, and separately on a dispatch page containing the dispatch information. Another method includes printing both the information 60 and the dispatch information together on contiguous paper, optionally between starting and ending messages, and so forth. An alternative special mathematical association method is discussed hereinbelow.

Typically, the authenticator 70 is relatively secure, such that the various devices and the authentication information elements enclosed therein can be assumed to be unchangeable. For example, the authenticator 70 can be enclosed within a password protected sealed electronic

box which, if opened without authorization, may disable the normal operation of the authenticator 70, or may clearly indicate that it has been tampered with.

As mentioned hereinabove, the authenticator 70 can form part of the sending transceiver 42. Fig. 3 illustrates such an embodiment, which is similar to that of Fig. 2 and similar functional elements have similar reference numerals.

In Fig. 3, the input unit 72 of the sending transceiver 42 comprises means, for example a serial, parallel or disk interface, for inputting the information 60 and the destination address 62 from any component of the sending transceiver 42, for example from its input devices. The sending transceiver 42 replaces the transceiver 76 of Fig. 2. The storage unit 54 however is optional, as the information 60 and the related dispatch information could be provided to the output unit 58 "on-the-fly" in a manner similar to that used by the "copy" function of document facsimile machines.

Generally, in various embodiments of the authenticator 70, the information 60 can be obtained from any source and by any means, including a computer, a disk drive, a scanner or any other component of the sending transceiver 42, a communication line, a communication network and any combinations thereof, and so forth.

Furthermore, any information element having information content the substance of which is equivalent to that of the transmitted information can serve for authentication purposes, regardless of its form, representation, format or resolution, whether it is a paper document or electronic information, whether digital or analog, whether in form of dots and lines or alphanumeric, binary, hexadecimal and other characters, and so forth. The element may contain additional information which does not change the substance and its content, such as a logo, a header message, etc. Furthermore, it may contain control, handshake and even noise data.

For example, if the materials 40 provided for transmission are paper documents, one embodiment of the authenticator 70 authenticates the original documents by printing the dispatch information on them.

Optionally, additional dispatch information may be provided to, or generated by authenticator 70, such as the number of pages transmitted, page numbers, the sender's identification, the sending transceiver's 42 identification, the receiving transceiver's 46 identification, the transmission elapsed time, a transmission identifier, integrity information such as a cyclic redundancy code (CRC), a checksum or the length of the transmitted

information, an authenticator identification indication such as a serial number, a verification from the communication network 44 that the transmission has actually taken place at the specified time from the sender to the recipient's address, a heading message, a trailing message and so forth.

Typically, when the authenticator 70 comprises a reasonably secure storage unit 54, the stored information is retained therein and copies thereof are provided to the output unit 58. Preferably, the provided output or any part thereof is reasonably secured, so as to prevent any fraudulent action. For example, if the output is a printout, it can be secured by spreading invisible or other ink on it, or by using special ink, special print fonts or special paper to print the authentication information, or in any other suitable manner. Another method includes securing the dispatch information using, for example, an encryption technique, and printing the encrypted information on the printout. At a later stage the encrypted information can be decrypted to provide the true dispatch information, and so forth. Likewise, mathematical association method as discussed hereinbelow can also be used.

It will be appreciated that the following embodiments fall within the scope of the present invention:

The authenticator of the present invention can operate for information, such as a document produced by a word processor, transmitted through a computer. In this embodiment, the computer may include the secure time generator (which may for example be externally plugged into the parallel port). The authenticator obtains the dispatch information from the transceiver, and the document is provided from the hard disk or word processing program. The authenticator encrypts the document and the dispatch information together and stores them in a file. When authentication is required, the authenticator retrieves the stored file, decrypts it and provides the document and the dispatch information associated therewith to a printer.

Similarly, information transmitted in a computer network or electronic mail system can be authenticated, for example, by having a file server or mail manager (equipped with a secure time generator) store the transmitted information together with its associated dispatch information in a secure manner. One embodiment of secure storage is that which has read-only privileges.

The present invention can be operated in conjunction with a message transmission forwarding service such as that provided by Graphnet Inc. of Teaneck, New Jersey, USA. The

service obtains the information and address from the sender, typically by an electronic transmission, occasionally converts it (for example from ASCII text or word processor format into a transmissible document format) and forwards it to the requested address. The forwarding service serves as the authenticator and may for example provide the dispatch information associated with the transmitted information to the sender in a secure manner, such as in a sealed envelope.

An efficient method for associating a plurality of electronic (digital) information elements is mathematical association. A digital information element can be represented as a number, for example as the element's standard binary, hexadecimal or other base representation. Using mathematical association, rather than maintaining the information elements (numbers) themselves, it is sufficient to maintain the results (also numbers) of one or more functions which are applied to one or more of these information elements. (These results are sometimes referred to as "message-digests", "hash-values" or "digital-signatures"). More formally, if A is a set of information elements, and F is the mathematical association function, then the set B of information elements is obtained as the result of applying the function F to the set A of information elements, i.e. B=F(A).

Preferably, the function F is selected such that a fraudulent attempt to change the elements of the set A, or an attempt to claim that a set A' which comprises different elements is the original set, can be readily detected by comparing the result B' obtained by applying the function F to the set A', to the original result B, i.e. by checking if F(A')=F(A).

Various function classes of various degrees of complexity can be used for mathematical association purposes in accordance with various embodiments of the present invention. Furthermore, the function F and/or the result B can be kept secret and unknown in general, and to interested parties such as the sender or the recipient in particular. However, even if the function F and/or the result B are known, the task of finding a meaningful different set A' such that B=F(A') is mostly very difficult even for relatively simple functions, not to mention for more complex ones.

A special class of functions most suitable for the purposes of the present invention is the class of functions having the property that given the result B = F(A), it is exceptionally difficult to find a second set A' such that applying the function F to the second set A' will yield the same result B. The term "exceptionally difficult" refers herein to the fact that although many different such sets A' may exist, it is so difficult to find even one of them

(sometimes even to find the set A itself) that it is practically infeasible. In fact, the functions of this class "hide" the elements they are applied to, (and sometimes the elements even cannot be reconstructed) and therefore this class is referred to herein as "the Hiding Class".

There are many advantages to using mathematical association in general, and functions of the Hiding Class in particular:

(a) It is efficient, for example for saving storage space and transmission bandwidth, to maintain a function result, the size of which is normally very small compared to the information elements themselves which can be arbitrarily large.

(b) It provides security, since the result is cryptic and there is no need to secure the information elements themselves. Furthermore, it is difficult, and sometimes infeasible to reconstruct the original elements.

(c) It provides a clear indication as to the authenticity of the elements of the set A used by the function to generate the result B. At any later time, the result B' of applying the function F to a purported set A' can be compared to the original result B, and a match indicates beyond any reasonable doubt that set A' is same as the original set A. Moreover, integrity information such as the length of the information elements of the set A can be added and used as part of the set A, or the results of a plurality of functions can be maintained such that to make the task of finding such a different set A' infeasible.

(d) The result B' provided for comparison must be equal to the original result B, since any change to A will yield a different result B' with very high probability, and even if by chance a different set A' is found for which F(A')=B, the chance that it will be meaningful or will have the same length is practically zero.

(e) The function can be selected such that it is relatively easy and fast to compute the function result.

Two well known and widely used functions of the Hiding class are encryption functions (e.g. the RSA algorithm) and Cyclic-Redundancy-Check (C.R.C.) functions (e.g. the C.R.C-32 function). While C.R.C functions are generally used in applications requiring verification as to the integrity of an arbitrarily long block of data, encryption is used to maintain the original data elements, though in different, cryptic representation. Encryption functions convert the information elements into one or more cryptic data blocks using one key, while enabling their reconstruction by providing another key. Other well known members of this class of functions

in the prior art are compression functions (e.g. the Lempel-Ziv 1977 and 1978 algorithms) and one-way hash functions (e.g. the MD2, MD4, and MD5 algorithms).

Description of the MD5 algorithm can be found in "One-Way Hash Functions," (B. Schneier, Dr. Dobb's Journal M&T Publishing Inc., September 1991 Vol 16 No.9 p148(4)) and in the Internet Request For Comments (RFC) document 1321. The MD4 algorithm is described in "The MD4 Message Digest Algorithm" (R. L. Rivest, Crypto '90 Abstracts, Aug. 1990, pp. 301-311, Springer-Verlag). Other publications relating to encryption, public-key cryptography and to cryptography and data security in general include: "Untangling Public-Key Cryptography" (B.Schneier, Dr. Dobb's Journal, M&T Publishing Inc., May 1992 Vol 17 No. 5 p16 (8)), " The Digital Signature Standard proposed by the National Institute of Standards and Technology" (Communications of the ACM, ACM Inc., July 1992 Vol 35 No. 7 p36(5)), "SHA: the Secure Hash Algorithm", (Stallings, William, Dr. Dobb's Journal, M&T Publishing Inc., April 1994 v19 n4 p32 (2)), and "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (Rivest, R.L., A. Shamir, and L. Adelman, Communications of the ACM, ACM Inc., February 1978 Vol 21 No. 2 pp. 120-126).

Description of the Lempel-Ziv 1977 compression algorithm can be found in "A Universal Algorithm for Sequential Data Compression" (Ziv. J., Lempel A., IEEE Transactions On Information Theory, Vol 23, No. 3, pp. 337-343).

Description of C.R.C. algorithms can be found in "Cyclic Redundancy Checksums (Tutorial)" (Louis, B. Gregory, C Users Journal, R & D Publications Inc., Oct 1992 v10 n10 p55 (6)), and in "File verification using C.R.C." (Nelson, Mark R., Dr. Dobb's Journal, M&T Publishing Inc., May 1992 Vol 17 No. 5 p64(6)).

The references and publications described by the above-mentioned articles are incorporated herein by reference.

Occasionally, there is no need to maintain the original information elements, and therefore the use of encryption functions (which normally maintain the information - though in a cryptic representation) may be disadvantageous. C.R.C functions (and other functions of the Hiding Class), on the other hand, maintain a small sized result value, but the information elements from which the result has been produced cannot be reconstructed therefrom. It would be more advantageous, for example, to apply a C.R.C. function to the union of all the information elements, i.e. to a bit-string, where the leftmost bit is the leftmost bit of the first

element, and the rightmost bit is the rightmost bit of the last element. This produces a cryptic and secure result, as described hereinabove. Furthermore, the C.R.C. function can be computed relatively quickly and easily.

Generally and more formally, the result B is a set of one or more information elements b1,...,bm, where each element bi (which itself can comprise one or more information elements) is the result of applying a (possibly different) function Fi to a subset Si of a set A which comprises one or more information elements a1,...,an, where the various subsets Si are not necessarily disjoint or different, each subset Si includes at least a portion of one or more (or even all) of the electronic information elements of the set A, and where each function Fi can comprise one or more functions (i.e. Fi can be the composition of functions). Preferably, the functions Fi are members of the Hiding Class. The elements of such a subset Si are considered to be mathematically associated.

Assuming that the set A comprises five information elements a1,a2,a3,a4,a5, a few examples of mathematical association function Fi and their result set B follow:

(the UNION function is denoted as U(x1,...,xk), which is an information element comprising a bit-string, where the leftmost bit is the leftmost bit of the element x1, and the rightmost bit is the rightmost bit of the element xk.)

(a) single element result set B

b1=F1(S1)=F1(a1,a4,a5) = a1/(a4+a5+1)

b1=F1(S1)=F1(a1,a3,a4) = ENCRYPT(U(a1,a3,a4))

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = MD5(U(a1,a2,a3,a4,a5)) * C.R.C(a3) mod 5933333

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = C.R.C(ENCRYPT(U(a1,a2)), COMPRESS(U(a2,a3,a4)), a1, a5)

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = U(a1,a2,a3,a4,a5) mod p (where p is a large Prime number)

(b) multi-element result set B

B = [C.R.C(U(a1,a3)), a2/(a1+1), ENCRYPT(a5)]

b1=F1(S1)=F1(a1,a3) = C.R.C(a1,a3)

b2=F2(S2)=F2(a1,a2) = a2/(a1+1)

b3=F3(S3)=F3(a5) = ENCRYPT(a5)

The elements of two or more (not necessarily disjoint) subsets of set A can be associated with each other by associating the elements of the result set B which correspond to these

subsets, either mathematically, or by non-mathematical methods, as described hereinabove. Furthermore, if there is a subset of elements of set A to which no function has been applied, these elements may be associated with the elements of the result set B, again either mathematically or by non-mathematical methods.

Moreover, the elements of two or more subsets of the set A can be associated with each other by associating the elements of each of these subsets with a common subset comprising one or more elements of the set A, where this common subset uniquely relates to the specific dispatch. This type of association is referred to herein as "indirect association", and the elements of this common subset are referred to herein as "link elements". A link element can be for example a unique dispatch number, or the subset comprising the time indication and a machine serial number, etc.

For example, assuming that the element a2 of the above set A uniquely relates to the dispatch, the following function generates a multi-element result set B:

B = [b1,b2,b3] = [ENCRYPT(a1, a2), COMPRESS(a2,a3,a4), a2+a5]

where the subsets Si include the following elements: S1=[a1,a2], S2=[a2,a3,a4] and S3=[a2,a5]. The elements of each subset are mathematically associated. Since all of these subsets include the common link-element a2, all their elements (in this case all the elements of the set A) are associated with each other.

Reference is now made to Fig. 4 which is a block diagram that illustrates an authenticator 100, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator 100 comprises a secure time generator 104, a storage device 106 and a function executor 102 which has means for inputting the following information elements: the transmitted information, the destination address, a time indication generated by the secure time generator 104, and a dispatch completion indication. Optionally, additional information elements can be provided as well.

The function executor 102 can be for example a Microchip Technology Inc.'s PIC16C5x series EPROM-based microcontroller, and the input means can be for example an I/O port, a serial, parallel or disk interface. The function executor 102 is capable of executing a function F on at least one, and preferably on the union of all of the input elements, and of generating a result information element which is provided to a storage device 106, and optionally to an output device 108, such as a printing device.

Preferably, the function F is a member of the Hiding Class, and is kept unknown at least to any interested part, by the function executor 102. This can be achieved for example by enabling the code protection feature of the PIC16C5x series microcontroller. Also, preferably the storage device 106 is a WORM device, such as a PROM. Preferably, a different function is used for each device employing the function F.

In accordance with one embodiment of the present invention, the authenticator further comprises a verification mechanism for verifying the authenticity of a set of information elements purported to be identical to the original set of information elements. It is however appreciated that the verification mechanism can be separated therefrom.

Reference is now made to Fig. 5 which is a block diagram that illustrates a verification mechanism 120, constructed and operative in accordance with a preferred embodiment of the present invention, where at least part of the information elements were mathematically associated by the authenticator 100 of Fig. 4.

The verification mechanism 120 includes a function executor 122 for generating a new result information element according to the same function employed by the function executor 102 of Fig. 4. The function executor 122 has means for inputting information elements corresponding to the original information elements input to the function executor 102 of Fig. 4., and which are purported to be identical to those original elements.

The verification mechanism 120 also comprises a comparator 124, which has input means for inputting the newly generated result information element and the original result information element which may be obtained from the storage device 106 of Fig. 4, or manually, for example through a keyboard. The comparator 124 then compares the two provided result information elements to determine if they are the same, and the comparison result can be output for example to a display or printing unit. A match indicates that the purported information elements are authentic.

Reference is now made to Fig. 6 which is a block diagram that illustrates a verification mechanism 140, constructed and operative in accordance with a preferred embodiment of the present invention, where the information elements were associated non-mathematically, and are for example stored in storage unit 54 by the authenticator 70 of Fig. 2.

The verification mechanism 140 comprises a comparator 144, which has input means for inputting at least one of the stored associated information elements from the storage unit 54 of Fig. 2. The comparator 124 also has input means for inputting the corresponding

information elements purported to be identical to the stored elements. The comparator 124 then compares the corresponding information elements to determine if they are the same, and the comparison result can be output for example to a display or printing unit. A match of all the compared elements indicates that the purported information elements are authentic.

It is appreciated that various embodiments of the present invention can include a combination of the verification mechanisms described hereinabove.

Also, part of the securing methods which were described for Fig. 2 include for example encryption and compression - methods which formally relate to mathematical association functions such as ENCRYPT(a1,...,aj) and COMPRESS(a1,...,aj). Occasionally, there is a need for reconstructing some or all of the secured mathematically associated information elements, for example for providing them to an output unit or to the comparator of the verification mechanism. Since some compression and encryption functions (as some other functions) are reversible, they are typically used when reconstruction of the elements is needed. (A function G is considered reversible if there exists a function H such that H(G(x))=x, and the function H is called the inverse function of G).

As discussed hereinabove, a mathematical association function can generally comprise a single function, or the composition of two or more functions. For example, the function ENCRYPT(a1,...,aj) comprises a single function - ENCRYPT, which is reversible, and its inverse function is DECRYPT. Another function COMPRESS(ENCRYPT(a1),C.R.C(a2,...,aj)) is the composition of three functions - COMPRESS, ENCRYPT and C.R.C, where the first two are reversible and their inverse function are DECOMPRESS (which yields the set comprising ENCRYPT(a1) and C.R.C(a2,...,aj)), and DECRYPT (which yields the element a1) respectively. The C.R.C function however, is not reversible.

Formally, if a function Fi comprises one or more functions, some of which are reversible, a set C comprising one or more information elements c1,...,ck can be generated, where this set C is expressive as a function I applied to the result information element bi of the function Fi, where this function I comprises the inverse function of one or more of these reversible functions.

While the present invention has been described with reference to a few specific embodiments, the description is illustrative of the invention and is not to be construed as limiting the invention. Various modifications may occur to those skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.

CLAIMS

1. Apparatus for providing a sender with authentication of the fact that certain information has been transmitted via a dispatcher to an address of a recipient, the apparatus comprising:

means for providing a set A comprising a plurality of information elements a1,...,an, said information element a1 having information content the substance of which is equivalent to that of said transmitted information, and said one or more information elements a2,...,an having dispatch information, where at least one of said information elements is provided in a reliable manner; and

means for associating at least a subset of said dispatch information elements a2,...,an with said information element a1, such that said associated information is secured against fraudulent actions attempted at least by said interested party, in a manner that such actions are at least detectable.

2. Apparatus according to claim 1, wherein said means for associating comprises means for generating a new set B comprising one or more information elements b1,...,bm, each element bi of said new set B being expressive as a function Fi of a subset Si comprising at least a portion of at least one electronic information element of said set A, and where said functions Fi can be different.

3. Apparatus according to claim 2, wherein said means for associating further comprises means for associating at least one information element of said new set B, with at least one information element of said set A.

4. Apparatus according to any of claims 2-3, wherein said set B comprises a plurality of elements, and wherein said means for associating further comprises means for associating at least two elements of said set B.

5. Apparatus according to claim 2, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si of said set A and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e. such that Fi(S')=bi.

6. Apparatus according to claim 2, wherein said function Fi comprises one or more functions.

7. Apparatus according to claim 2, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said interested party.

8. Apparatus according to any of claims 2 and 6, wherein said function Fi comprises at least one reversible function, and further comprising means for generating a set C comprising one or more information elements c1,...,ck expressive as a function I of at least said information element bi, where said function I comprises the inverse function of at least one of said reversible functions.

9. Apparatus according to any of claims 1-2, and further comprising means for verifying the authenticity of a set V1 comprising one or more information elements which are purported to be identical to the corresponding elements of a subset V2 comprising information elements of said set A, said verification means comprising:

means for providing said purported information elements of said set V1;

means for providing said information elements of said subset V2; and

means for comparing said purported information elements of said set V1 with said corresponding information elements of said subset V2 to determine if they are the same.

10. Apparatus according to claim 2, and further comprising means for verifying the authenticity of a set V3 comprising one or more information elements which are purported to be identical to the corresponding elements of said subset Si of said set A, said verification means comprising:

means for providing said purported information elements of said set V3;

means for generating a new information element bi' being expressive as said function Fi applied to said purported information elements of said set V3;

means for providing an information element bi" selected from the group comprising said new element bi, and an information element purported to be identical to said new element bi; and

means for comparing said elements bi' and bi" to determine if they are the same.

11. Apparatus according to any of claims 9-10, wherein said means for verifying is separated therefrom.

12. Apparatus according to any of claims 1-2, and further comprising means for providing, at least to an interested party, at least one information element of the group comprising said associated information elements and the elements of said set B.

13. Apparatus according to any of claims 1-2, and further comprising means for storing at least one information element of the group comprising said associated information elements and the elements of said set B.

14. Apparatus according to any of claims 1-2, and further comprising means for securing at least one information element of the group comprising said associated information elements and the elements of said set B.

15. Apparatus according to claim 1 and wherein said dispatch information includes at least one element of the group comprising the following elements: the date associated with said transmission, the time associated with said transmission, the address associated with said transmission, and a completion indication associated with said transmission.

16. Apparatus according to any of claims 1 and 15 and wherein said dispatch information includes at least one element of the group comprising the following elements: the number of pages transmitted, page number, indication of said sender identification, indication of said recipient identification, said transmission duration, integrity information, indication of said transmission identification, indication of said authentication apparatus identification, a heading message, and a trailing message.

17. Apparatus according to claim 1 wherein said information elements have form selected from the group comprising the following forms: a paper document and electronic information.

18. Apparatus according to any of claims 1 and 17 wherein said information element a1 is provided from a source selected from a group comprising the following elements: a paper document and electronic information.

19. Apparatus according to claim 18 wherein said information element a1 is said source.

20. Apparatus according to any of claims 1 - 2 and wherein said dispatch information includes at least one link information element, wherein said means for associating comprises means for associating said link information element with at least one of said information elements, and for associating it with at least one another information element.

21. Apparatus according to any of claims 1, 15 , 16 and 20, and further comprising means for preparing at least one of said information elements.

22. Apparatus according to claim 21 and further comprising a time indication generator which provides at least one of said time and said date associated with said transmission, where said time indication cannot be set or modified at least by an interested party.

23. Apparatus according to claim 1 wherein said dispatcher includes at least one element of the following group: a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, and a communication network.

24. Apparatus according claim 1 and further comprising means for providing said transmitted information to said dispatcher.

25. Apparatus according to claim 1 and wherein said apparatus is part of said dispatcher.

26. Apparatus according to claim 1 and wherein said apparatus is relatively secure, such that any fraudulent action can at least be detected.

27. A method for providing a sender with authentication of the fact that certain information has been transmitted via a dispatcher to an address of a recipient, the method comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, said information element a1 having information content the substance of which is equivalent to that of said transmitted information, and said one or more information elements a2,...,an having dispatch information, where at least one of said information elements is provided in a reliable manner; and

having an authenticator associate at least a subset of said dispatch information elements a2,...,an with said information element a1, such that said associated information is secured against fraudulent actions attempted at least by said interested party, in a manner that such actions are at least detectable.

28. A method according to claim 27 and wherein said dispatch information includes at least one element of the group comprising the following elements: the date associated with said transmission, the time associated with said transmission, the address associated with said transmission, and a completion indication associated with said transmission.

29. A method according to any of claims 27 and 28 and wherein said dispatch information includes at least one element of the group comprising the following elements: the number of pages transmitted, page number, indication of said sender identification, indication of said recipient identification, said transmission duration, integrity information, indication of said transmission identification, indication of said authentication apparatus identification, a heading message, and a trailing message.

30. A method according to claim 27 and wherein said information element a1 is provided from a source selected from a group comprising the following elements: a paper document and electronic information.

31. A method according to claim 30 wherein said information element a1 is said source.

32. A method according to claim 27 wherein said dispatcher includes at least one element of the following group: a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, and a transmission service.

33. A method according to claim 27 and further comprising the step of providing said transmitted information to said dispatcher.

34. A method according to any of claims 27 and 32, and wherein said authenticator is selected from a group comprising an independent, non-interested third party, said transmission service, a device, and any combination thereof.

35. A method for providing a sender with authentication of the fact that paper documents have been dispatched via a dispatch service to an address of a recipient, the method comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, said information element a1 having information content the substance of which is equivalent to that of said dispatched document, and said one or more information elements a2,...,an having dispatch information, where at least one of said information elements is provided in a reliable manner; and

having an authenticator associate at least a subset of said dispatch information elements a2,...,an with said information element a1, such that said associated information is secured against fraudulent actions attempted at least by said interested party, in a manner that such actions are at least detectable.

36. A method according to claim 35 and wherein said dispatch information includes at least one element of the group comprising the following elements: the date associated with said dispatch, the time associated with said dispatch, the address associated with said dispatch, and a completion indication associated with said dispatch.

37. A method according to any of claims 35 and 36 and wherein said dispatch information includes at least one element of the group comprising the following elements: the number of pages dispatched, page number, indication of said sender identification, indication of said

recipient identification, said dispatch duration, integrity information, indication of said dispatch identification, indication of said authentication apparatus identification, a heading message, and a trailing message.

38. A method according to claim 35 wherein said information element a1 is a copy of said dispatched documents.

39. A method according to claim 38, and further comprising the step of preparing said copy.

40. A method according to claims 35 wherein said dispatching service is selected from the following group: a courier service and the registered mail service of the post office.

41. A method according to claim 35 and further comprising the step of providing said dispatched documents to said dispatch service.

42. A method according to claim 35, and wherein said authenticator is selected from a group comprising an independent, non-interested third party, said dispatch service, a device, and any combination thereof.

43. A method according to any of claims 27 and 35, wherein said step of associating comprises the step of generating a new set B comprising one or more information elements b1,...,bm, each element bi of said new set B being expressive as a function Fi of a subset Si comprising at least a portion of at least one electronic information element of said set A, and where said functions Fi can be different.

44. A method according to claim 43, wherein said step of associating further comprises the step of associating at least one information element of said new set B, with at least one information element of said set A.

45. A method according to any of claims 43-44, wherein said set B comprises a plurality of elements, and wherein said step of associating further comprises the step of associating at least two elements of said set B.

46. A method according to claim 43, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si of said set A yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e. such that Fi(S')=bi.

47. A method according to claim 43, wherein said function Fi comprises one or more functions.

48. A method according to claim 43, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said interested party.

49. A method according to any of claims 43 and 47, wherein said function Fi comprises at least one reversible function, and further comprising the step of generating a set C comprising one or more information elements c1,...,ck expressive as a function I of at least said information element bi, where said function I comprises the inverse function of at least one of said reversible functions.

50. A method according to any of claims 27, 35, and 43, and further comprising the step of verifying the authenticity of a set V1 comprising one or more information elements which are purported to be identical to the corresponding elements of a subset V2 comprising information elements of said set A, said verification step comprising the steps of:

providing said purported information elements of said set V1;

providing said information elements of said subset V2; and

comparing said purported information elements of said set V1 with said corresponding information elements of said subset V2 to determine if they are the same.

51. A method according to claim 43, and further comprising the step of verifying the authenticity of a set V3 comprising one or more information elements which are purported to be identical to the corresponding elements of said subset Si of said set A, said verification step comprising the steps of:

providing said purported information elements of said set V3;

generating a new information element bi' being expressive as said function Fi applied to said purported information elements of said set V3;

providing an information element bi" selected from the group comprising said new element bi, and an information element purported to be identical to said new element bi; and

comparing said elements bi' and bi" to determine if they are the same.

52. A method according to any of claims 27, 35, and 43, and further comprising the step of providing to an interested party at least one information element of the group comprising said associated information elements and the elements of said set B.

53. A method according to any of claims 27, 35, and 43, and further comprising the step of storing at least one information element of the group comprising said associated information elements and the elements of said set B.

54. A method according to any of claims 27, 35, and 43, and further comprising the step securing at least one information element of the group comprising said associated information elements and the elements of said set B.

55. A method according to any of claims 27, 35, and 43, and wherein said dispatch information includes at least one link information element, wherein said step of associating comprises the step of associating said link information element with at least one of said information elements, and the step of associating it with at least one another information element.

56. A method according to any of claims 27 and 35, and further comprising the step of preparing at least one of said information elements.

57. A method according to any of claims 27 and 35, wherein said information elements have form selected from the group comprising the following forms: a paper document and electronic information.

58. A method according claim 27, and further comprising the step of transmitting said information to said address of said recipient.

59. A method according to claim 35, and further comprising the step of dispatching said documents to said address of said recipient.

ABSTRACT

Apparatus and method for providing a sender with authentication of the fact that certain information has been transmitted via a dispatcher to an address of a recipient is disclosed. The method includes the steps of: a) providing a set A comprising a plurality of information elements a1,...,an, the information element a1 having information content the substance of which is equivalent to that of the transmitted information, and the one or more information elements a2,...,an having dispatch information, where at least one of the information elements is provided in a reliable manner and b) associating at least a subset of the dispatch information elements a2,...,an with the information element a1, such that the associated information is secured against fraudulent actions attempted at least by the interested party, in a manner that such actions are at least detectable. The apparatus implements the operations of the method.

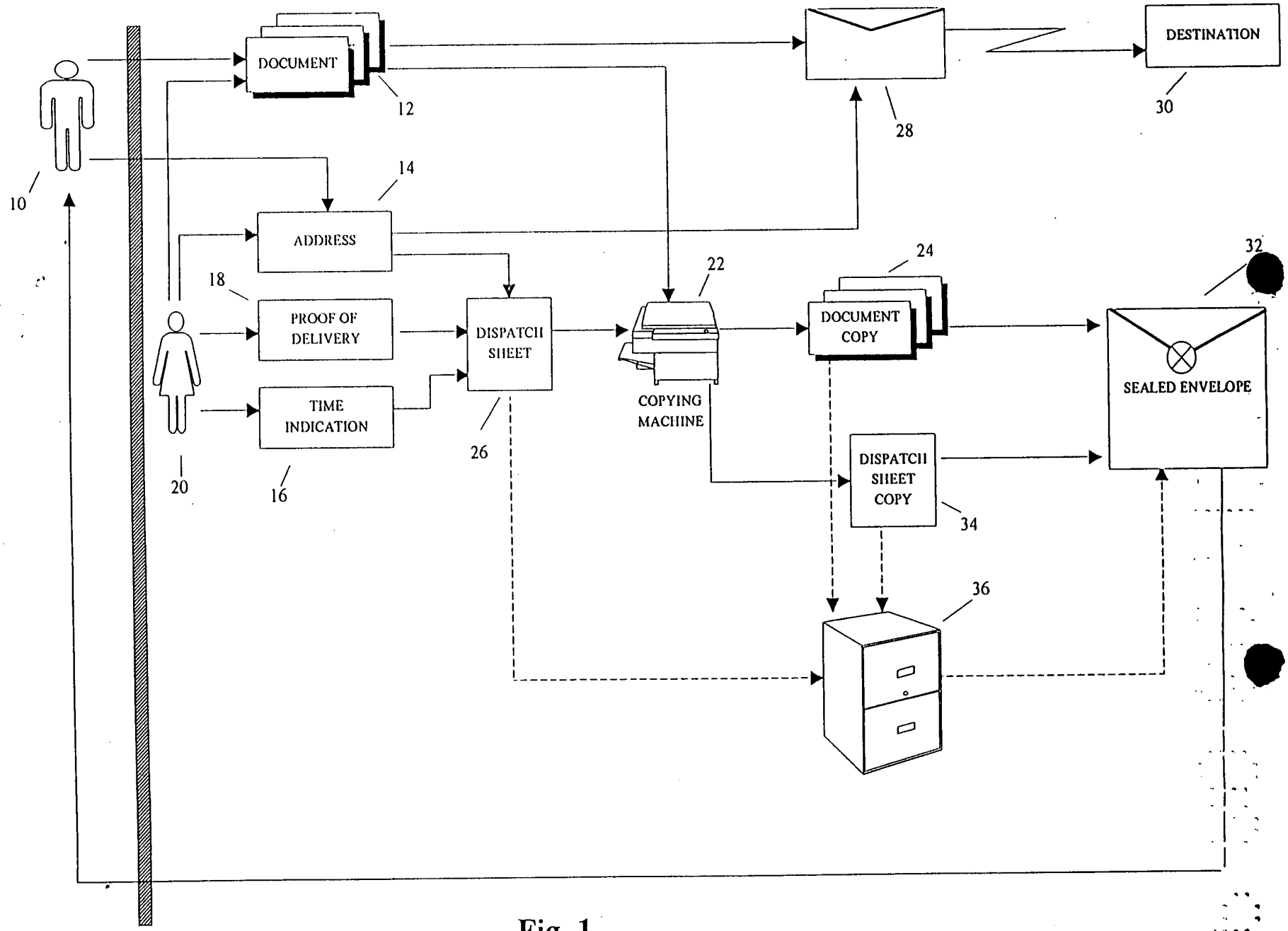

DOCUMENT
12
DESTINATION
30
28
10
14
ADDRESS
18
PROOF OF DELIVERY
TIME INDICATION
20
16
DISPATCH SHEET
26
22
COPYING MACHINE
24
DOCUMENT COPY
32
SEALED ENVELOPE
DISPATCH SHEET COPY
34
36

Fig. 1

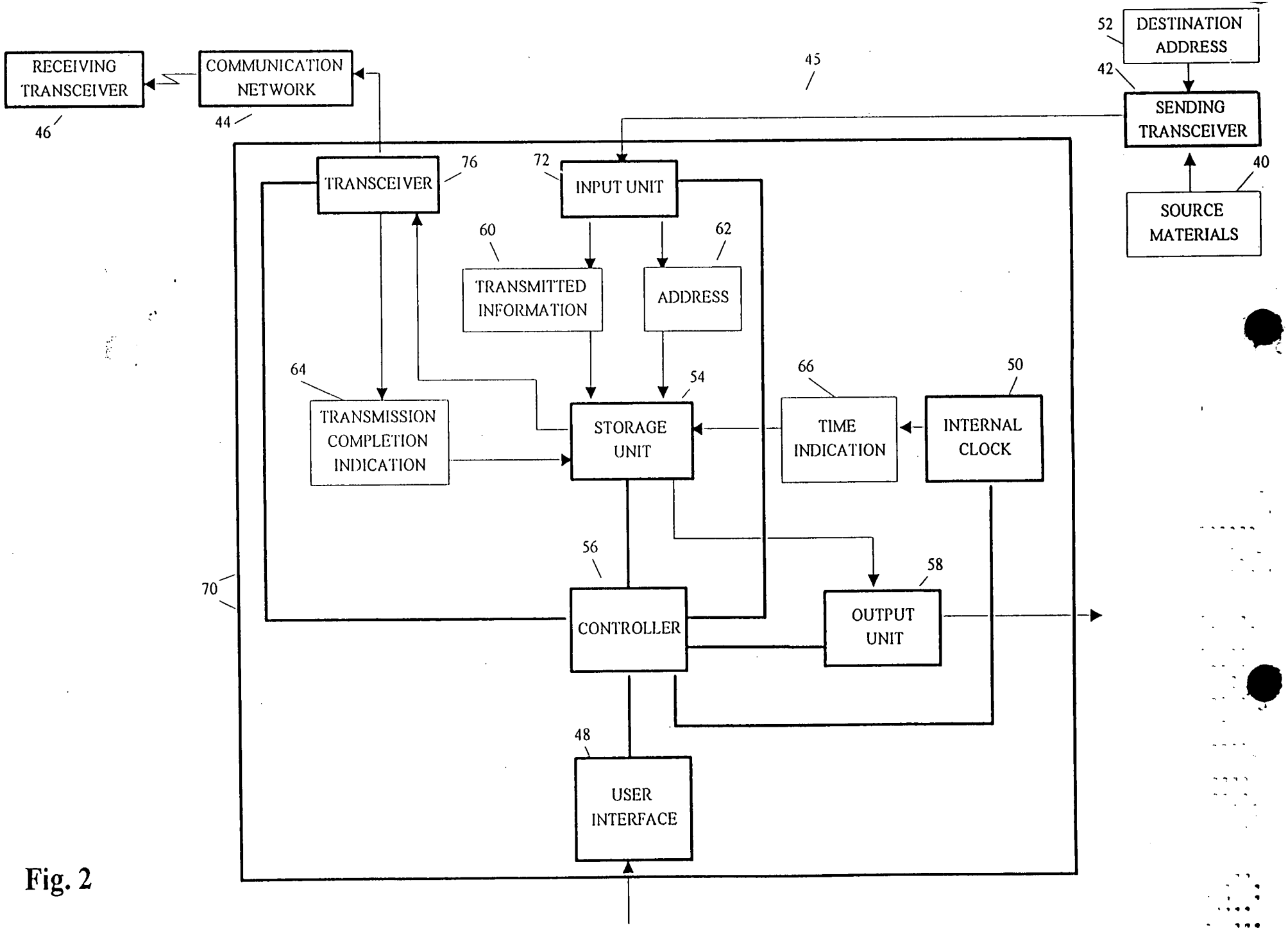

RECEIVING TRANSCEIVER
46
COMMUNICATION NETWORK
44
45
52
DESTINATION ADDRESS
42
SENDING TRANSCEIVER
40
SOURCE MATERIALS
TRANSCEIVER
76
72
INPUT UNIT
60
TRANSMITTED INFORMATION
62
ADDRESS
64
TRANSMISSION COMPLETION INDICATION
54
STORAGE UNIT
66
TIME INDICATION
50
INTERNAL CLOCK
56
CONTROLLER
58
OUTPUT UNIT
70
48
USER INTERFACE

Fig. 2

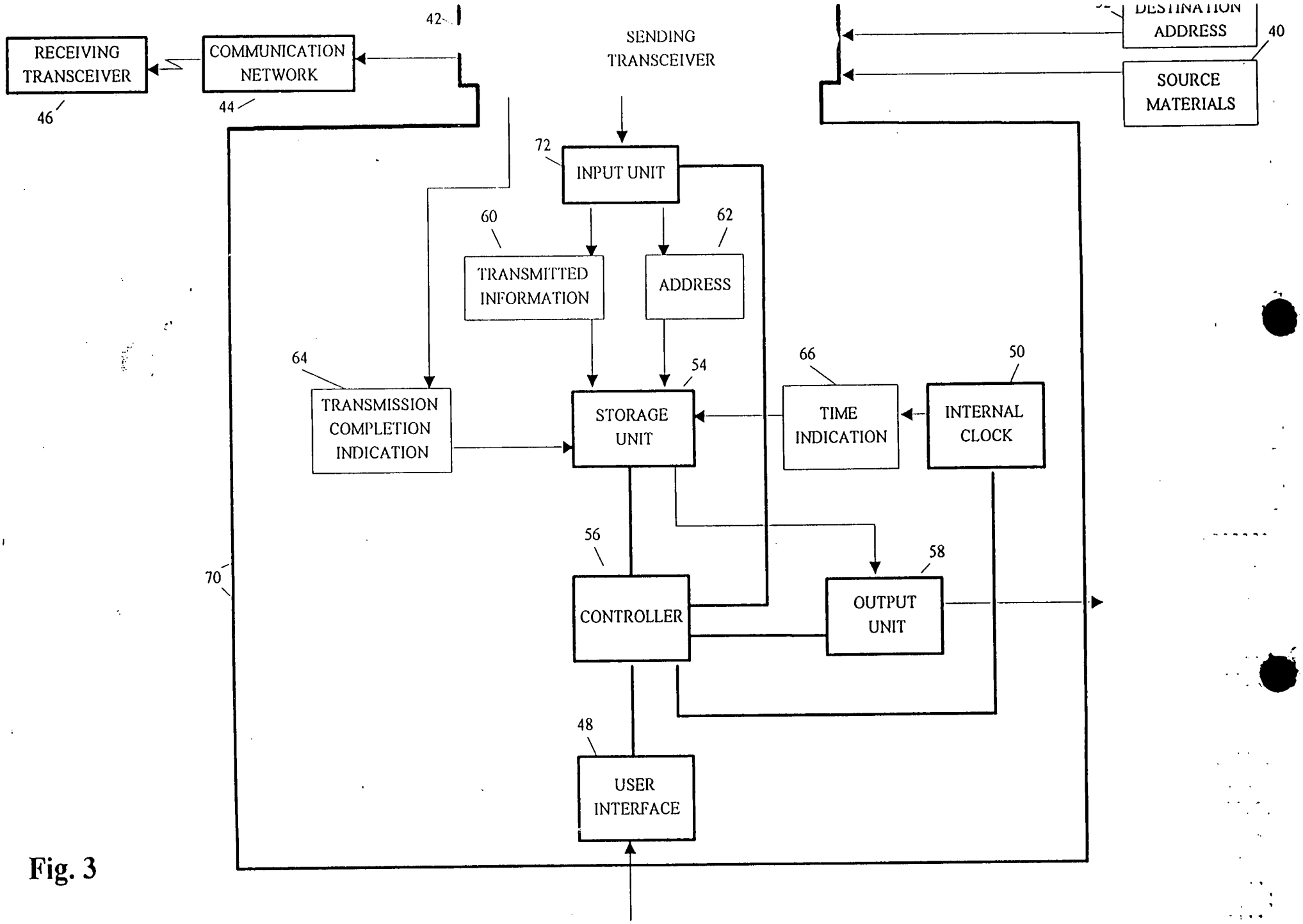

RECEIVING TRANSCEIVER
46
COMMUNICATION NETWORK
44
42
SENDING TRANSCEIVER
DESTINATION ADDRESS
40
SOURCE MATERIALS
72
INPUT UNIT
60
TRANSMITTED INFORMATION
62
ADDRESS
64
TRANSMISSION COMPLETION INDICATION
54
STORAGE UNIT
66
TIME INDICATION
50
INTERNAL CLOCK
56
CONTROLLER
58
OUTPUT UNIT
70
48
USER INTERFACE

Fig. 3

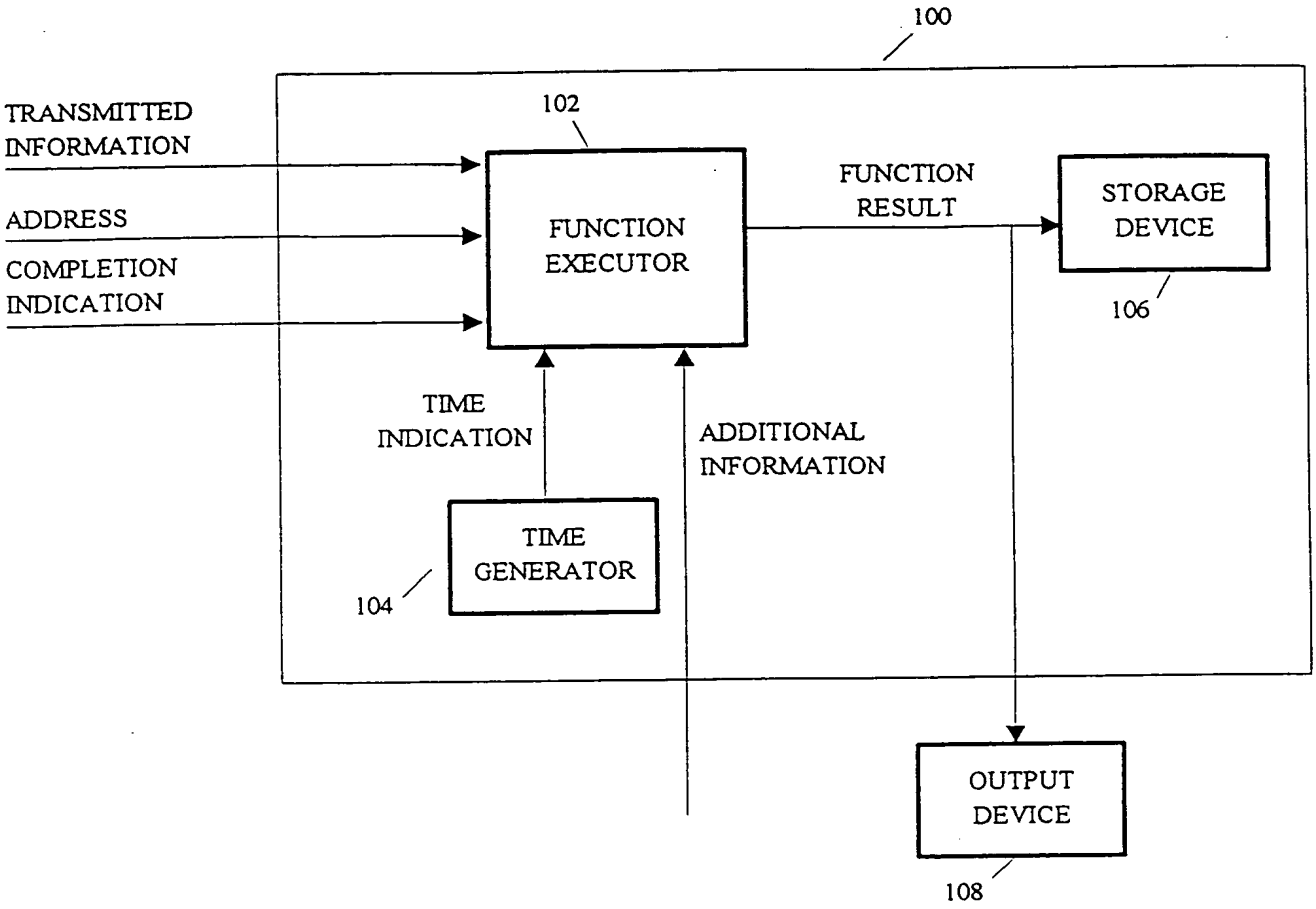

100
TRANSMITTED INFORMATION
ADDRESS
COMPLETION INDICATION
102
FUNCTION EXECUTOR
FUNCTION RESULT
STORAGE DEVICE
106
TIME INDICATION
ADDITIONAL INFORMATION
TIME GENERATOR
104
OUTPUT DEVICE
108

FIG. 4

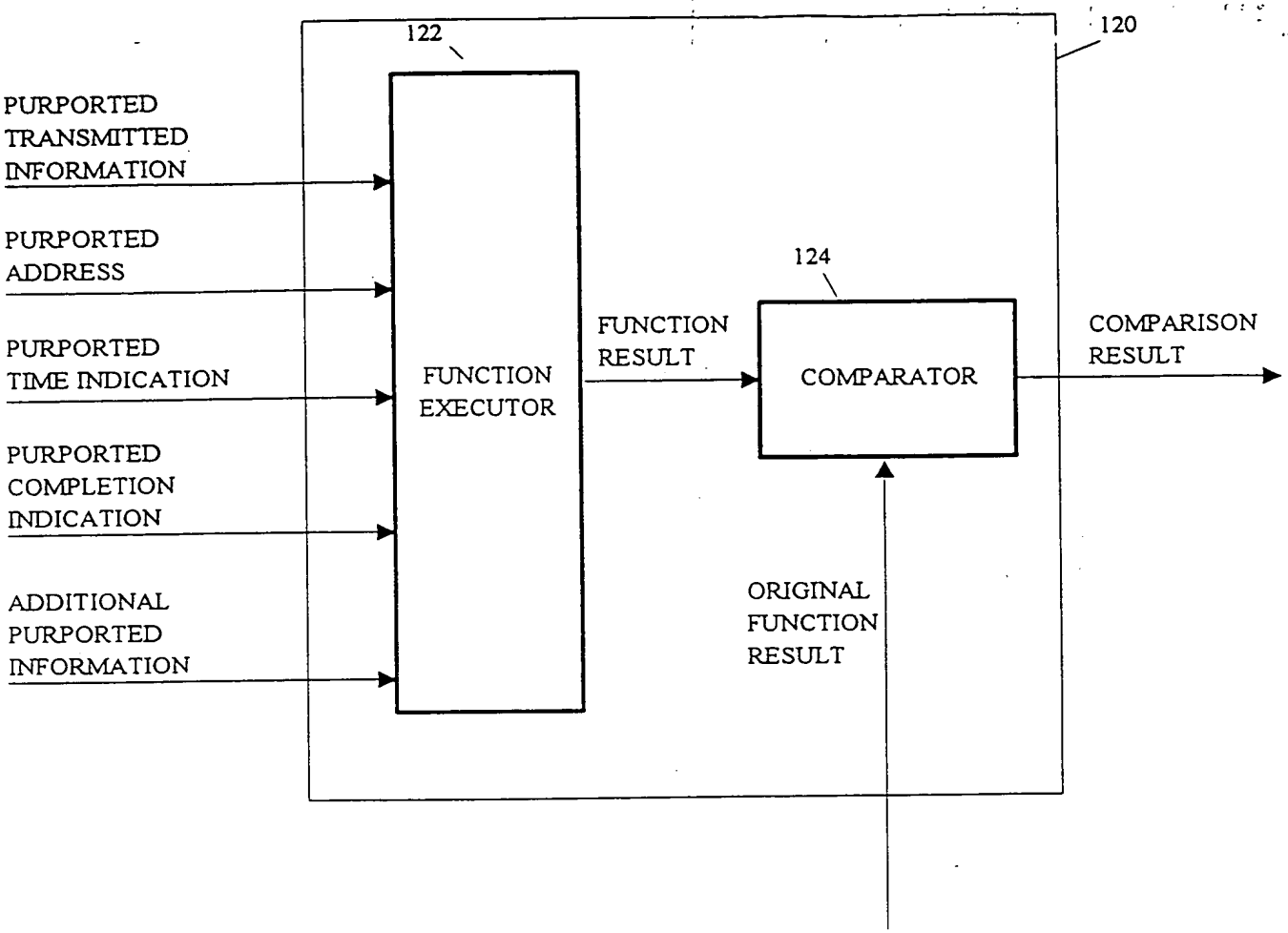
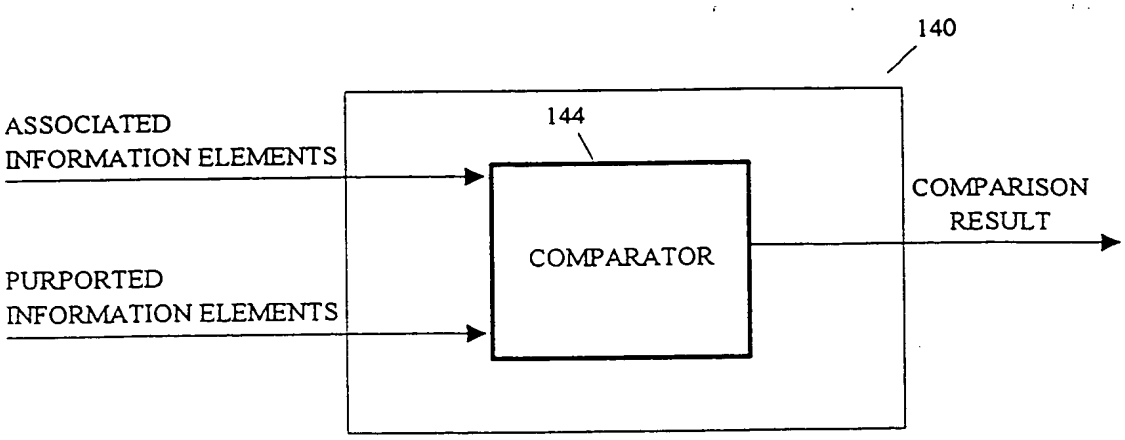

122
120
PURPORTED TRANSMITTED INFORMATION
PURPORTED ADDRESS
PURPORTED TIME INDICATION
PURPORTED COMPLETION INDICATION
ADDITIONAL PURPORTED INFORMATION
FUNCTION EXECUTOR
FUNCTION RESULT
124
COMPARATOR
COMPARISON RESULT
ORIGINAL FUNCTION RESULT

FIG. 5


140
144
ASSOCIATED
INFORMATION ELEMENTS
PURPORTED
INFORMATION ELEMENTS
COMPARATOR
COMPARISON
RESULT

6/6

FIG. 6